Office of Inspector General

March 2008
Report No. AUD-08-006

FDIC's Replacement and Disposal Process for Laptop Computers

AUDIT REPORT

Office of Audits

OIG

Office of Audits

Federal Deposit Insurance Corporation

Report No. AUD-08-006 **March 2008**

FDIC's Replacement and Disposal Process for Laptop Computers

Why We Did The Audit

The objective of the audit was to determine whether the FDIC had established and implemented adequate controls over the replacement and disposal process for laptop computers.

Background

During 2007, the FDIC purchased 3,905 Lenovo T60 Thinkpad laptop computers and related hardware for a total cost of approximately $7.8 million. The new laptops would provide FDIC employees with faster system/software performance, extended battery life, increased disk storage space, and a larger display screen. In addition, the new laptops include *Pointsec for PC* (Pointsec) encryption software to enhance the security of corporate data. The FDIC's Division of Information Technology (DIT) was responsible for the 2007 laptop deployment project.

FDIC Circular 1380.3, *Laptop Computer Assignments, Safeguards, and Asset Management*, dated April 1999, establishes policies and procedures for managing FDIC-owned laptop computers throughout their life cycle. In addition, in July 2007, DIT issued *Guidelines for New Laptop Deployment* (DIT Guidelines), which provides detailed procedures for the replacement and disposal of laptops, including procedures for the disposition of the hard drives from used laptops in order to protect sensitive data they may contain.

An inventory of laptop computers owned by the FDIC is maintained in the FDIC's Remedy® Asset Management Module. DIT used Remedy® to track the deployment of the new laptop computers and the collection of used laptops.

Audit Results

The FDIC established and implemented generally adequate controls over the replacement and disposal process for laptop computers. Specifically, we noted that the FDIC had implemented a consistent and complete deployment of laptop computers during 2007 in each of the offices we reviewed. Further, DIT personnel at each location we visited maintained documentation in accordance with the DIT Guidelines. All 3,905 laptop computers purchased by the FDIC were received and recorded in the FDIC's Remedy® laptop inventory within the timeframes established by DIT. Finally, as stipulated in the new laptop purchase order, the FDIC received a discount for its used laptop computers.

We also found that opportunities exist for the FDIC to enhance controls for the continuous replacement and disposal process for laptop computers in the following areas. It is important to note that the FDIC will continue to replace malfunctioning computers.

- FDIC Circular 1380.3 does not reflect the current business environment for managing the FDIC's laptop computer inventory and does not define the FDIC's policy for the disposal of laptop computer hard drives. This limits the FDIC's assurance that its laptop computer inventory, including hard drives that may contain sensitive information, are effectively managed.

- Current hard drive destruction practices present a risk that a computer hard drive could be lost and subject to unauthorized access.

- Remedy® lacks sufficient access controls to ensure that complete and accurate inventory records are maintained for the FDIC's laptop computers and does not track replacement laptops for malfunctioning computers. These control deficiencies limit the FDIC's assurance regarding the integrity of its laptop computer inventory.

Recommendations and Management Response

We recommended that FDIC management (1) update Circular 1380.3 to reflect the FDIC's current business environment for managing its laptop computer inventory and to define policy for the disposal of hard drives; (2) implement additional measures that mitigate the risk of a computer hard drive being lost during the destruction process and subject to unauthorized access; and (3) establish procedures to track and record the replacement of laptop computers returned to the vendor for replacement or service. Management concurred with our recommendations and is taking responsive corrective actions.

To view the full report, go to www.fdicig.gov/2008reports.asp

Contents *Page*

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226

Office of Audits
Office of Inspector General

DATE: March 12, 2008

MEMORANDUM TO: Michael E. Bartell
Chief Information Officer and
Director, Division of Information Technology

/Signed/
FROM: Russell A. Rau
Assistant Inspector General for Audits

SUBJECT: *FDIC's Replacement and Disposal Process for Laptop Computers* (Report No. AUD-08-006)

This report presents the results of the subject audit. The FDIC's Division of Information Technology (DIT) was responsible for the 2007 laptop computer deployment project to upgrade the FDIC's laptop computer inventory. The objective of the audit was to determine whether the FDIC had established and implemented adequate controls over the replacement and disposal process for laptop computers. We conducted this performance audit in accordance with generally accepted government auditing standards. Appendix 1 of this report discusses our audit objective, scope, and methodology in detail.

BACKGROUND

Under a contract with SRA International, Inc. (SRA), the FDIC purchased 3,905 Lenovo T60 Thinkpad laptop computers and related hardware from World Wide Technology, Inc. (WWT) for a total cost of approximately $7.8 million. The new laptop computers provide FDIC employees with faster system/software performance, extended battery life, increased disk storage space, and a larger display screen. In addition, the new laptop computers were deployed with *Pointsec for PC* (Pointsec)[1] encryption software to enhance the security of corporate data. Under the laptop computer purchase order, the FDIC received a discount for trading in its used laptop computers, without the hard drives.

[1] Pointsec encrypts all data on the laptop computer's hard drive as a safeguard in the event the laptop is lost or stolen.

A record of all laptop computers owned by the FDIC is maintained in Remedy®,[2] which also includes the assignment history of the laptops. DIT used Remedy® to track the deployment of the new laptop computers and the collection of the used laptops.

Guidance Related to Laptop Computers

DIT Guidelines on Laptops. In July 2007, DIT issued *Division of Information Technology Guidelines for New Laptop Deployment* (DIT Guidelines), which provides detailed procedures for the replacement and disposal of laptop computers. The DIT Guidelines also provide procedures for the storage and destruction of the hard drives from used laptops in order to protect sensitive data the hard drives may contain. Specifically, the DIT Guidelines state that the DIT Distribution Center (DDC) is responsible for ensuring that used laptop computer hard drives are destroyed by shredding. At the time of our audit, DDC personnel were destroying laptop computer hard drives by transporting them to a suburban Washington, D.C., recycling facility where the hard drives were placed into an automobile that was then crushed and fed into an industrial shredding machine (see Figure 1 below). DDC personnel are to remain on-site to witness the shredding.

Figure 1: Hard Drive Destruction at the Recycling Facility

Source: OIG observation of the hard drive destruction at the recycling facility.

FDIC Policies and Procedures Related to Laptops. The FDIC has established the following policies and procedures that relate to the replacement and disposal process for laptop computers:

- FDIC Circular 1380.3, *Laptop Computer Assignments, Safeguards, and Asset Management*, dated April 13, 1999, establishes policies and procedures for managing FDIC-owned laptop computers throughout their life cycle.

[2] Remedy® consists of a suite of applications used for incident, problem change, service-level, and asset management. DIT uses the Asset Management Module of Remedy® to track laptop computers.

- FDIC Circular 3200.1, *Disposition of Corporation-Owned Property*, dated August 25, 2004, establishes procedures for ensuring that Corporation-owned property is reallocated and/or disposed of in a uniform and effective manner; and

- FDIC Circular 1360.9, *Protecting Sensitive Information*, dated April 30, 2007, establishes policy on protecting sensitive information stored on FDIC laptop computers.

Federal Law and Guidelines. The following summarizes federal guidance related to the destruction of laptop computer hard drives.

- *The Federal Information Security Management Act of 2002* (FISMA) defines federal agency responsibilities for information security, including assessing risks associated with, among other things, the unauthorized access to information systems, which includes information technology (IT) equipment. [3] This provision of FISMA requires that federal agencies develop, document, and implement policies and procedures that cost-effectively reduce such information security risks to an acceptable level.

- The National Institute of Standards and Technology (NIST) issued guidelines that federal agencies should consider in relation to information system security.[4] NIST Special Publication (SP) 800-88, *Guidelines for Media Sanitization*, dated September 2006, provides guidelines for organizations to make practical sanitization decisions based on the level of confidentiality of their sensitive information. NIST SP 800-88 recommends the destruction of hard drives containing sensitive information by disintegrating, shredding, pulverizing, or incinerating. Additionally, NIST SP 800-53 Revision 1, *Recommended Security Controls for Federal Information Systems*, dated December 2006, recommends among other things, that organizations employ appropriate sanitization techniques for their information system media.

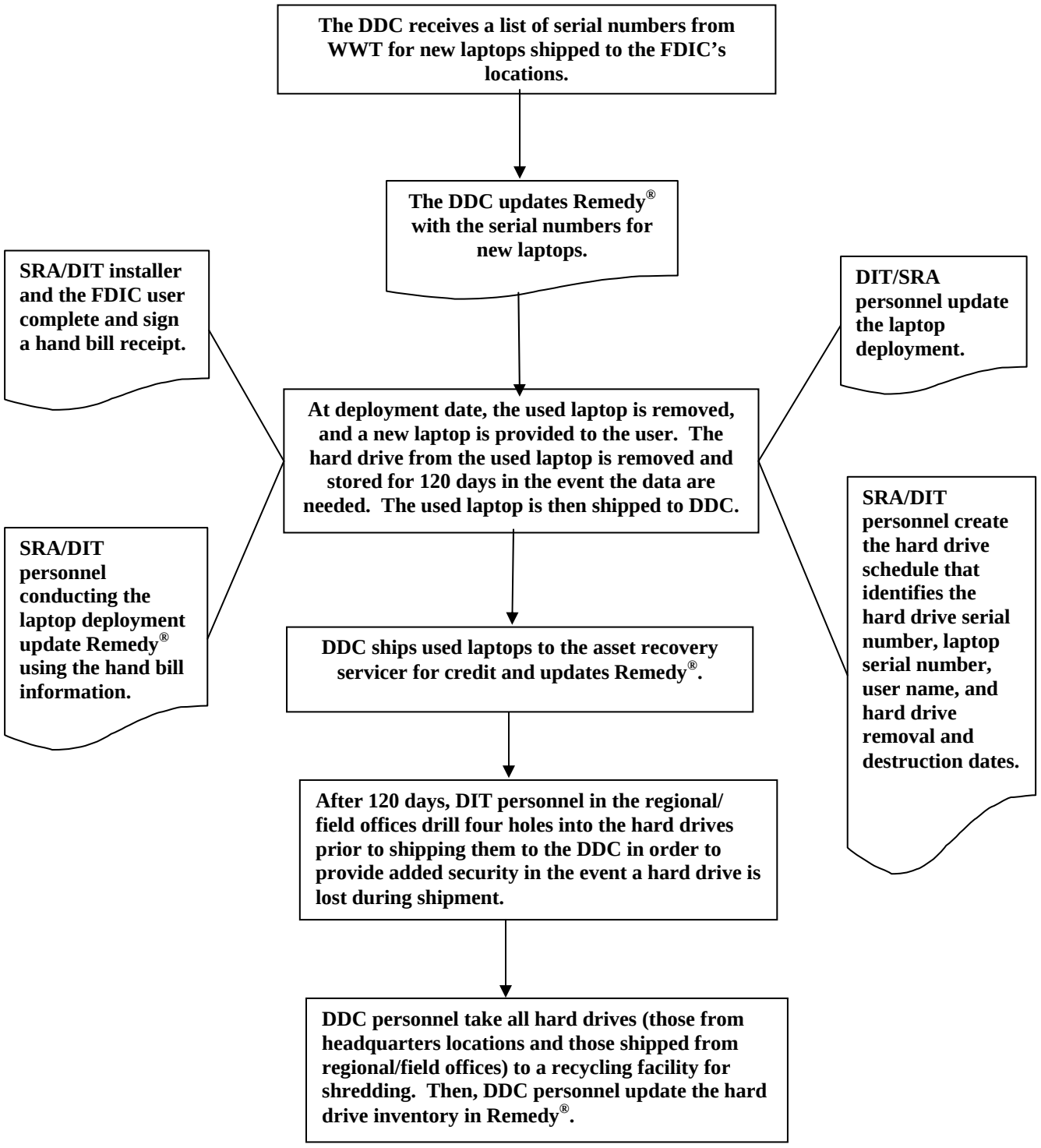
The FDIC's Laptop Deployment Process

The FDIC's laptop computer deployment process consisted of retrieving used laptops from FDIC users, migrating user data, configuring new laptops, and removing hard drives from the used laptops. DIT developed a laptop computer deployment schedule using Remedy®, which identified users at each FDIC site. At the FDIC's headquarters buildings,[5] DIT oversaw the laptop computer deployment, which was conducted by SRA personnel. DIT personnel conducted the laptop computer deployment at the FDIC's

[3] The FDIC has determined that the provision of FISMA at issue here is legally binding on the FDIC.
[4] NIST special publications are, by their own terms, guidelines (rather than mandatory requirements) for agencies in implementing their IT operations.
[5] Headquarters includes two buildings in Washington, D.C., and the Virginia Square buildings in Arlington, Virginia.

regional and field offices. Figure 2 below further illustrates the FDIC's 2007 replacement and disposal process for laptop computers.

Figure 2: The FDIC's 2007 Replacement and Disposal Process for Laptop Computers



RESULTS OF AUDIT

The FDIC established and implemented generally adequate controls over the replacement and disposal process for laptop computers. Specifically, we noted that the FDIC had implemented a consistent and complete deployment of laptop computers during 2007 in each of the offices we reviewed and that DIT personnel at each location we visited maintained documentation in accordance with the DIT Guidelines.[6] In addition, all 3,905 laptop computers purchased by the FDIC were received and recorded in the FDIC's Remedy® laptop inventory within the timeframes established by DIT. Further, as stipulated in the new laptop purchase order, the FDIC received a discount for its used laptop computers. Such results are positive. However, opportunities exist for the FDIC to enhance its controls for the continuous replacement and disposal process for laptop computers (see the table below). It is important to note that the FDIC will continue to replace malfunctioning computers.

Summary of Control Enhancements Needed

Control Issue	Enhancement Needed
FDIC Circular 1380.3, *Laptop Computer Assignments, Safeguards, and Asset Management*, does not reflect the FDIC's current procedures for managing laptop computers, including hard drives, or DIT's current business environment. In addition, Circular 1380.3 does not define the FDIC's policy for the disposal of laptop computer hard drives. The lack of current policies and procedures in these areas limits the FDIC's assurance that its laptop computer inventory, including hard drives that may contain sensitive information, are effectively managed (**FDIC Policies and Procedures for Managing the Laptop Computer Inventory**).	Update Circular 1380.3 to reflect the FDIC's current business environment for managing its laptop computer inventory and to define policy for the disposal of hard drives.
Current hard drive destruction practices present a risk that a computer hard drive could be lost and subject to unauthorized access (**Hard Drive Destruction Practices**).	Implement additional measures that mitigate the risk of a computer hard drive being lost during the destruction process and subject to unauthorized access.
Remedy® lacks sufficient access controls to ensure that complete and accurate inventory records are maintained for the FDIC's laptop computers. Further, Remedy® does not track replacement laptops for malfunctioning computers. These control deficiencies limit the FDIC's assurance regarding the integrity of its laptop computer inventory (**The FDIC's Asset Management Module**).	Implement access controls and establish Remedy® procedures to track and record the replacement of laptop computers returned to the vendor for service.

[6] We tested the laptop computer deployment process at FDIC locations in Arlington, Virginia; Washington, D.C.; Atlanta, Georgia; New York, New York; Chicago, Illinois; and Madison, Wisconsin.

FDIC POLICIES AND PROCEDURES FOR MANAGING THE LAPTOP COMPUTER INVENTORY

The FDIC issued Circular 1380.3, *Laptop Computer Assignments, Safeguards, and Asset Management*, dated April 13, 1999, for the purpose of establishing policies and procedures for all FDIC-owned laptop computers throughout their life cycle. However, the circular does not reflect the FDIC's current business environment for managing its laptop computer inventory. In addition, Circular 1380.3 does not define the FDIC's policy for the disposal of laptop computer hard drives. The lack of current policies and procedures in these areas limits the FDIC's assurance that its laptop computer inventory, including hard drives that may contain sensitive information, are effectively managed.

Changes in the FDIC's Business Environment and Procedures for Managing Laptop Computers

Circular 1380.3 does not reflect the FDIC's current business environment or procedures for managing laptop computers. For example, Circular 1380.3:

- References the Information Technology Asset Management System (ITAMS) as the FDIC's laptop inventory system. However, ITAMS was replaced by Remedy® in June 2004.

- Requires that all laptops moved in and out of FDIC facilities be inspected by FDIC security personnel. However, according to FDIC Security and Emergency Preparedness officials, this practice has been discontinued for FDIC employees.

- Requires equipment authorization tags to be fastened to the outside of laptop computer cases and to be visible at all times. However, this practice is no longer employed.

- Assigns the responsibility for periodic and annual inventories nationwide to the Chief, Logistics Management Section, to ensure the accuracy of inventory records for all FDIC-owned laptops. However, this position no longer exists, and no other FDIC circular assigns this responsibility.

- References the Division of Information Resources Management (DIRM), which was restructured as DIT in 2005.

Laptop Computer Hard Drives

The DIT Guidelines that were developed specifically for the 2007 replacement and disposal of laptop computers contain detailed procedures to safeguard hard drives removed from laptop computers. However, Circular 1380.3 does not address the FDIC's policy for the disposal of hard drives. During our review of the 2007 laptop deployment, DIT officials informed us that ensuring control over hard drives was a major concern because of sensitive information they may contain. The FDIC can achieve greater assurance regarding the disposal of computer hard drives and promote adherence to NIST security guidelines by addressing the disposal of hard drives in corporate policy.

Recommendation on FDIC Policies and Procedures for Managing the Laptop Computer Inventory

We recommend that the Chief Information Officer (CIO):

(1) Update Circular 1380.3 to reflect the FDIC's current business environment for managing its laptop computer inventory and to define policy for the disposal of hard drives.

HARD DRIVE DESTRUCTION PRACTICES

DIT disposed of laptop computer hard drives from the 2007 laptop deployment effort by transporting them to a suburban Washington, D.C., recycling facility for destruction. However, many of the hard drives had not been drilled, as a security precaution, prior to their transport to the recycling facility, presenting a risk that a computer hard drive could be lost during the destruction process and subject to unauthorized access.

Current Destruction Process for Hard Drives

Consistent with FISMA, NIST Special Publication 800-53 Revision 1, *Recommended Security Controls for Federal Information Systems*, recommends that organizations employ appropriate sanitization techniques for their information system media to prevent the disclosure of organizational information to unauthorized individuals when such media are reused or disposed of.

On January 15, 2008, we accompanied an SRA employee to the recycling facility to observe the destruction of approximately 200 laptop computer hard drives. According to the SRA employee, these hard drives were from FDIC headquarters, regional, and field offices. DIT Guidelines require that hard drives from regional and field offices be drilled prior to shipment to the DDC. However, DIT Guidelines do not require that hard drives removed from laptops in headquarters offices be drilled prior to being transported for shredding. The destruction process at the recycling facility involved placing the

computer hard drives into cardboard boxes and then placing the boxes into an automobile that was about to be destroyed. An industrial crane was then used to compact the automobile and transport it to a conveyer belt, which then fed the automobile into an industrial shredder. However, as the automobile was being transported to the conveyer belt, we observed what appeared to be hard drives falling out of the automobile onto a large trash heap in the recycling facility's scrap yard. Because many of the hard drives had not been drilled prior to being placed in the automobile, there is a risk that one or more of them may not have been destroyed and could be lost and subject to unauthorized access.

Plans for Destroying Additional Hard Drives

DIT recently deployed Pointsec, which automatically encrypts sensitive information stored on laptop computer hard drives. Pointsec significantly reduces the risk of a compromise of sensitive information whenever a laptop computer is lost or stolen. However, the computer hard drives destroyed on January 15, 2008 were removed from laptop computers that did not have the automatic encryption software. As a result, these laptop computer hard drives may have contained sensitive information in an unencrypted format. DIT plans to destroy a large number of other laptop computer hard drives, in the near future, that may also contain sensitive information in an unencrypted format. Accordingly, DIT should implement additional measures to mitigate the risk of a computer hard drive being lost during the destruction process and subject to unauthorized access. In this manner, the FDIC can reduce the risk of an unauthorized disclosure of sensitive information that could lead to potential legal liability or public embarrassment to the Corporation.

Recommendation on Hard Drive Destruction Practices

We recommend that the CIO:

(2) Implement additional measures that mitigate the risk of a computer hard drive being lost during the destruction process and subject to unauthorized access.

THE FDIC's ASSET MANAGEMENT MODULE

The FDIC uses the Remedy® Asset Management Module to manage its inventory of laptop computers. However, Remedy® lacks sufficient access controls to ensure that complete and accurate inventory records are maintained for the FDIC's laptop computers. In addition, Remedy® does not track replacement laptop computers when a malfunctioning laptop, assigned to a user, is returned to the vendor for service. As a result, the FDIC cannot ensure the effective accountability for, and control of, laptop computers.

Data Controls in the Remedy® Inventory System

During the 2007 laptop computer deployment, personnel who conducted the laptop replacement had unrestricted access to the laptop asset record in Remedy®. Specifically, 13 SRA employees in the FDIC's headquarters offices and at least 40 DIT personnel at FDIC regional and field offices could edit inventory records in Remedy® related to the laptop inventory without authorization or supervisory review. Further, DIT personnel in the regional and field offices stated that without their knowledge, inventory records could be modified by DIT personnel in Washington, D.C. NIST SP 800-53 Revision 1, *Recommended Security Controls for Federal Information Systems,*[7] dated December 2006, includes recommended security controls for federal information systems to enforce the separation of duties through assigned access authorizations.

To DIT's credit, it had identified concerns related to Remedy® and its IT asset inventory processes prior to our audit. To address these concerns, DIT contracted with an independent firm to conduct a review of the Corporation's IT asset management processes. The firm reported to DIT in January 2008,[8] that Remedy® does not contain adequate controls over changes in IT asset records. The report states that Remedy® roles should be restricted based on the principle of least privilege.[9] To compensate for the lack of access control, the firm recommended that asset record changes be saved and held pending supervisory review and approval. DIT officials informed us that they intend to implement corrective actions to address the firm's recommendations. Such actions would provide DIT management greater assurance regarding the integrity of the FDIC's laptop computer inventory. Therefore, we are not making recommendations related to this area.

Laptops Returned to the Vendor

FDIC Circular 1380.3 requires that current and accurate records for the receipt, transfer, disposal, and adjustment of laptop assignments be maintained. Although Remedy® tracks the status of laptop computer deployments, the system does not provide a link between a laptop returned to the vendor and the replacement laptop to ensure that laptop inventory records are accurate.

To illustrate, a laptop computer deployed to an FDIC employee would be coded as "deployed," and a laptop being stored by DIT for future use would be coded in Remedy® as "in inventory." Another code, "returned to vendor" was used for 426 FDIC laptops. According to DIT officials, a computer coded as "returned to vendor" indicates that the malfunctioning laptop was kept by the vendor and that the FDIC received a replacement laptop for which a separate record was created in the Remedy® inventory. However, Remedy® does not provide a crosswalk, for example, a code, to indicate which laptop the

[7] Although the FDIC's information systems do not fall within the SP 800-53 definition of federal information systems, we believe the guidance in that publication provides a best practice for the FDIC to consider in managing its information systems.
[8] The firm's report is entitled *FDIC IT Asset Analysis.*
[9] Under the principle of least privilege, the information system enforces the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks.

vendor provided as the replacement laptop. Therefore, the FDIC does not have the records to adequately assure that the FDIC received a replacement laptop for each computer that was coded "returned to vendor." DIT should establish procedures to track replacement laptop computers for those computers that have been returned to the vendor.

Recommendation on Procedures for Tracking Replacement Laptops

We recommend that the CIO:

(3) Establish procedures to track and record the replacement of laptop computers returned to the vendor for replacement or service.

CORPORATION COMMENTS AND OIG EVALUATION

On March 7, 2008, the CIO and Director, DIT, provided a written response to the draft of this report. Management's response is presented in its entirety in Appendix 2. Management concurred with our findings and recommendations.

In response to recommendation 1, DIT stated that it will revise Circular 1380.3 as part of a larger asset management documentation project. In response to recommendation 2, DIT has already advised the DDC that all hard drives must be rendered physically disabled prior to being sent off-site for shredding. Furthermore, DIT is updating the documentation on hard drive disposal for all equipment and updating procedures to render all hard drives inoperable prior to storage for disposal. In response to recommendation 3, DIT will develop procedures for tracking assets returned to the vendor and replacement assets sent to the FDIC.

A summary of management's response to the recommendations is in Appendix 3. DIT's planned actions are responsive to our recommendations. The recommendations are resolved but will remain open until we determine that the agreed-to corrective actions have been completed and are responsive.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The audit objective was to determine whether the FDIC had established and implemented adequate controls over the replacement and disposal process for laptop computers. We conducted this performance audit from September 2007 through January 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Scope and Methodology

The audit included an assessment of the FDIC's plans and procedures for the replacement and disposal of laptop computers during 2007. We conducted fieldwork at FDIC headquarters locations in Arlington, Virginia; and Washington, D.C.; FDIC regional and field offices in Atlanta, Georgia; New York, New York; and Chicago, Illinois, and one additional field office in Madison, Wisconsin. We conducted tests of the FDIC's laptop deployment for the FDIC's field offices in Eau Claire, Appleton, and Milwaukee, Wisconsin; and Shelby, Alabama.

To accomplish the audit objective, we performed the following:

- Reviewed various guidelines as follows:
  - *Division of Information Technology Guidelines for New Laptop Deployment*, dated July 2007.
  - FDIC Circular 3200.1, *Disposition of Corporation-Owned Property*, dated August 25, 2004.
  - FDIC Circular 1360.9, *Protecting Sensitive Information*, dated April 30, 2007.
  - FDIC Circular 1380.3, *Laptop Computer Assignments, Safeguards, and Asset Management*, dated April 13, 1999.
  - FISMA.
  - NIST SP 800-88, *Guidelines for Media Sanitization*, dated September 2006.
  - NIST SP 800-53 Revision 1, *Recommended Security Controls for Federal Information Systems*, dated December 2006.

- Interviewed FDIC employees and SRA contractors regarding the FDIC's procedures for the replacement and deployment of laptop computers.
- Verified the storage procedures for 100 percent of the hard drives at the locations noted earlier.
- Verified receipt of the 3,905 Lenovo T60 laptop computers, purchased under SRA Purchase Order 9010166, to the vendor's shipping confirmations.
- Reconciled the vendor's shipping confirmations for the 3,905 laptop computers to the FDIC's Remedy® inventory.
- Verified the completion of signed hand bills for the deployment of 500 judgmentally sampled laptops.
- Verified the accuracy of signed hand bills for the deployment of 100 judgmentally sampled laptops.
- Observed DIT's hard drive disposition procedures at FDIC regional and field offices.
- Reconciled hard drive inventory records to disposal records for used laptops.
- Reconciled documentation for used laptop shipments to with the FDIC's records.
- Verified background investigations for SRA personnel.
- Observed hard drive shredding procedures by the FDIC's DDC.
- Assessed DIT's procedures for tracking laptop computers returned to the vendor.

In addition, prior to our audit, DIT contracted for a review of the FDIC's IT asset inventory control process, including the verification of selected aspects of the IT asset inventory, such as the laptop computer inventory controls. Accordingly, we did not perform audit procedures already covered by that review.

Internal Control

We evaluated the effectiveness of controls in place for the replacement and disposal of laptop computers. These controls included policies and procedures contained in many of the documents listed above. In the absence of written policies, we relied on interviews with, and information obtained from, DIT officials.

DIT did not separately inventory the hard drives of the FDIC's laptop computers. The FDIC deployed Pointsec in 2007 to automatically encrypt sensitive information stored on laptop computer hard drives. Such software significantly reduces the risk of a compromise of sensitive information whenever a laptop computer is lost or stolen.

Reliance on Computer-processed Information

For purposes of the audit, we did not rely on computer-processed information to support our audit findings, conclusions, or recommendations. Our assessment centered on records related to the replacement and disposal of laptop computers and hard drives. In addition, DIT had contracted with an independent firm to test data and selected information systems controls in the Remedy® Asset Management Module, which contains an inventory of FDIC laptop computers. Accordingly, we did not consider it necessary to develop procedures to assess those controls.

Compliance with Laws and Regulations, Government Performance and Results Act, and Fraud or Abuse

We reviewed applicable laws and regulations related to the FDIC's replacement and disposal process for laptop computers. We found no instances where the FDIC was not in compliance with applicable laws and regulations, but we did note areas for improvement as described in the report.

We reviewed DIT's performance measures under the Government Performance and Results Act, Public Law 103-62. We also reviewed the FDIC's 2007 Annual Performance Plan, the FDIC's Strategic Plan for 2005-2010, and DIT's Balanced Scorecard to determine whether the FDIC has established goals related to its laptop replacement and disposal process. Neither the annual plan nor the strategic plans include goals, objectives, or indicators specifically related to the subject of our audit.

We assessed the risk of fraud and abuse related to the audit objective in the course of evaluating audit evidence.

CORPORATION COMMENTS

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226-3500
Division of Information Technology

MAR 0 7 2008

MEMORANDUM TO: Russell A. Rau, Assistant Inspector General for Audits
Office of Inspector General

FROM: Michael E. Bartell, CIO and Director
Division of Information Technology

SUBJECT: FDIC Response to the Draft Audit Report Entitled,
FDIC's Replacement and Disposal Process for Laptop Computers
(Assignment 2007-032)

Thank you for the opportunity to respond to the draft report entitled, *FDIC's Replacement and Disposal Process for Laptop Computers*. The Division of Information Technology (DIT) appreciates the professionalism of the FDIC Office of Inspector General (OIG) during this audit.

DIT concurs with the OIG's assessment that, "The FDIC has established and implemented controls over the replacement and disposal process for laptop computers that were generally adequate. Specifically, we noted that the FDIC had implemented a consistent and complete deployment of laptop computers during 2007 in each of the offices we reviewed. Further, DIT personnel at each location we visited maintained documentation in accordance with the DIT Guidelines. All 3,905 laptop computers purchased by the FDIC were received and recorded in the FDIC's Remedy® laptop inventory within the timeframes established by DIT. Finally, as stipulated in the new laptop purchase order, the FDIC received a discount for its used laptop computers."

DIT also concurs that additional opportunities exist to enhance our existing controls. As such, DIT has carefully considered each of the three OIG recommendations which suggest how the FDIC may further improve our policies, hard drive protection measures and our tracking procedures. The OIG draft report recommends that the CIO:

Recommendation #1:

Update Circular 1380.3 to reflect the FDIC's current business environment for managing its laptop computer inventory and to define policy for the disposal of hard drives.

Response: Concur. DIT is in the process of reviewing asset management documentation, which will include the Circular 1380.3 and the current procedures for equipment disposal. The update to 1380.3 is part of a larger asset management documentation project that was initiated in February 2008 to:

- identify all applicable current policies, directives, procedures, and processes and the associated gaps in this documentation;

- prioritize the efforts required to address identified documentation issues based on the current needs of the Asset Management Program; and
- complete the necessary document changes.

As part of this project, Circular 1380.3 will be revised to reflect the FDIC's current business environment for managing its laptop computer inventory and to define policy for the disposal of hard drives by 12/31/2008.

Recommendation #2:

Implement additional measures that mitigate the risk of a computer hard drive being lost or subject to unauthorized access during the destruction process.

Response: Concur. As part of the asset management documentation project, DIT is currently updating the documentation on drive disposal for all equipment. Specifically, DIT is reviewing and updating procedures to render all hard drives inoperable prior to storage for disposal. In the interim, DIT has already advised the DIT Distribution Center (DDC) that all hard drives must be rendered physically disabled prior to being sent off-site for shredding. The revised procedures will be completed by 4/15/2008.

Recommendation #3:

Establish procedures to track and record the replacement of laptop computers returned to the vendor for replacement or service.

Response: Concur. DIT will develop procedures for tracking assets returned to vendor and replacement assets sent back to the FDIC. This information will be added into the Asset Management Operations Manual by 8/31/2008.

cc: Rus Pittman (DIT)
Karen Keats (DIT)
Rack Campbell (DIT)
James Angel, Jr. (OERM)

MANAGEMENT RESPONSE TO RECOMMENDATIONS

This table presents the management response on the recommendations in our report and the status of the recommendations as of the date of report issuance.

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved: [a] Yes or No	Open or Closed [b]
1	DIT will revise Circular 1380.3 to reflect the FDIC's current business environment for managing its laptop computer inventory and to define policy for the disposal of hard drives.	Dec. 31, 2008	N/A	Yes	Open
2	DIT is updating the documentation on hard drive disposal for all equipment. Specifically, DIT is reviewing and updating procedures to state that all hard drives must be rendered inoperable prior to storage for disposal.	April 15, 2008	N/A	Yes	Open
3	DIT will develop procedures for tracking assets returned to the vendor and replacement assets sent to the FDIC.	August 31, 2008	N/A	Yes	Open

[a] Resolved - (1) Management concurs with the recommendation, and the planned corrective action is consistent with the recommendation.
(2) Management does not concur with the recommendation, but planned alternative action is acceptable to the OIG.
(3) Management agrees to the OIG monetary benefits, or a different amount, or no ($0) amount. Monetary benefits are considered resolved as long as management provides an amount.

[b] Once the OIG determines that the agreed-upon corrective actions have been completed and are responsive, the recommendation can be closed.